IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method for providing computer security, comprising:

determining, using a processor, whether an executable associated with a static state meets a predetermined criterion;

associating a first risk level with the executable, if it is determined that the executable meets the predetermined criterion;

observing that a process started by the executable has performed or has attempted to perform an action with which a second risk level, being a higher level than the first, is associated;

updating the first risk level to the [[a]] second risk level based on the observation ~~that is higher than the first risk level if a process started by the executable is observed to perform or attempt an action with which the second risk level is associated~~; and

performing a predetermined responsive action with respect to the process if the second risk level exceeds the threat detection threshold;

wherein determining whether the executable meets the predetermined criterion does not compare the executable with a virus signature.

2. (Previously Presented) The method for providing computer security as recited in Claim 1, wherein the risk level indicates a level of potential risk that will be brought by operating the executable.

3. (Previously Presented) The method for providing computer security as recited in Claim 1, wherein the risk level indicates how much risk the executable presents.

4. (Previously Presented) The method for providing computer security as recited in Claim 1, wherein the predetermined criterion includes a configuration criterion.

5. (Previously Presented) The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable is configured as a service.

6. (Previously Presented) The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable is configured to run under a highly privileged account.

7. (Previously Presented) The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable is installed via a standard procedure.

8. (Previously Presented) The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has sufficient access control.

9. (Previously Presented) The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable is modified.

10. (Previously Presented) The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable is signed.

11. (Previously Presented) The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has a modified date different from created date.

12. (Previously Presented) The method for providing computer security as recited in Claim 1, wherein the predetermined criterion includes a capability criterion.

13. (Previously Presented) The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has networking capability.

14. (Previously Presented) The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has privilege manipulation capability.

15. (Previously Presented) The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has remote process capability.

16. (Previously Presented) The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has process launching capability.

17. (Previously Presented) The method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has secure coding violation.

18. (Previously Presented) The method for providing computer security as recited in Claim 1, further comprising associating with the executable a risk type indicating a type of risk to which the executable is vulnerable.

19-28. (Cancelled)

29. (Previously Presented) The method for providing computer security as recited in Claim 1, further comprising analyzing historical evidence.

30. (Previously Presented) The method for providing computer security as recited in Claim 1, further comprising analyzing historical evidence, wherein the historical evidence includes a record of activities.

31. (Previously Presented) The method for providing computer security as recited in Claim 1, further comprising analyzing historical evidence, wherein the historical evidence includes a log file.

32. (Previously Presented) The method for providing computer security as recited in Claim 1, further comprising analyzing historical evidence, wherein the historical evidence includes a system optimization file.

33. (Previously Presented) The method for providing computer security as recited in Claim 1, further comprising analyzing historical evidence, wherein the historical evidence includes a crash dump file.

34. (Previously Presented) The method for providing computer security as recited in Claim 1, further comprising analyzing historical evidence, wherein the historical evidence includes a prefetch file.

35. (Previously Presented) The method for providing computer security as recited in Claim 1, further comprising performing a dynamic risk analysis.

36. (Previously Presented) The method for providing computer security as recited in Claim 1, further comprising determining whether an action is required.

37. (Currently amended) A system for providing computer security, comprising:

a processor configured to:

determine whether an executable associated with a static state meets a predetermined criterion;

associate a risk level with the criterion, if it is determined that the executable meets the predetermined criterion;

observe that a process started by the executable has performed or attempted to perform an action with which a second risk level, being a higher level than the first, is associated;

update the first risk level to the [[a]] second risk level based on the observation ~~that is higher than the first risk level if a process started by the executable is observed to perform or attempt an action with which the second risk level is associated~~; and

perform a predetermined responsive action with respect to the process if the second risk level exceeds the threat detection threshold;

wherein determining whether the executable meets a predetermined criterion does not compare the executable with a virus signature; and

a memory coupled with the processor, configured to provide the processor with instructions.

38. (Currently amended) A computer program product for providing computer security, the computer program product being embodied in a computer readable storage medium and comprising computer instructions for:

determining whether an executable associated with a static state meets a predetermined criterion;

associating a risk level with the criterion, if it is determined that the executable meets the predetermined criterion;

observing that a process started by the executable has performed or has attempted to perform an action with which a second risk level, being a higher level than the first, is associated;

updating the first risk level to the [[a]] second risk level based on the observation ~~that is higher than the first risk level if a process started by the executable is observed to perform or attempt an action with which the second risk level is associated~~; and

performing a predetermined responsive action with respect to the process if the second risk level exceeds the threat detection threshold;

wherein determining whether the executable meets a predetermined criterion does not compare the executable with a virus signature.